

Quantum key distribution

a new tool for the secure communications toolbox

Richard Hughes

Physics Division

Los Alamos National Laboratory

- Cryptographic key transfer by quantum (single-photon) communications
 - recent LANL ground-based experiments in free-space:
 - New Journal of Physics 4, 43 (2002): www.njp.org
 - feasibility of satellite QKD
 - Phys. Rev. Lett. 81, 3283 (1998)
 - Proc SPIE 4635, 116 (2002)
 - turbulence and photon counting
 - Proc. SPIE 5111, 7 (2003)
 - QKD in an all-optical network ?
 - PTL (to appear, Nov 2003)

LANL quantum key distribution team: June 2003



W. Marshall, J. Thrasher, N. Dallman, K. Tyagi, C. Wipf, P. Hiskett
R. Sedillo, S. Storms, J. Ettinger, **C. Peterson**, N. Olivas, P. Milonni, J. Anaya
J. Nordholt, R. Hughes, I. Medina, P. Montano, **K. McCabe**
(+ M. Neergaard, M. Pigue, R. Scarlett)

10-km free-space quantum key distribution

Richard Hughes, Jane Nordholt, Derek Derkacs and Charles Peterson

Sample of key material at 10-km range (day)

one-airmass path: comparable optics to satellite-to-ground

A: 01110001 01111010 00100001 01100100 10100110

B: 01110001 01111010 00100001 01100100 10100110

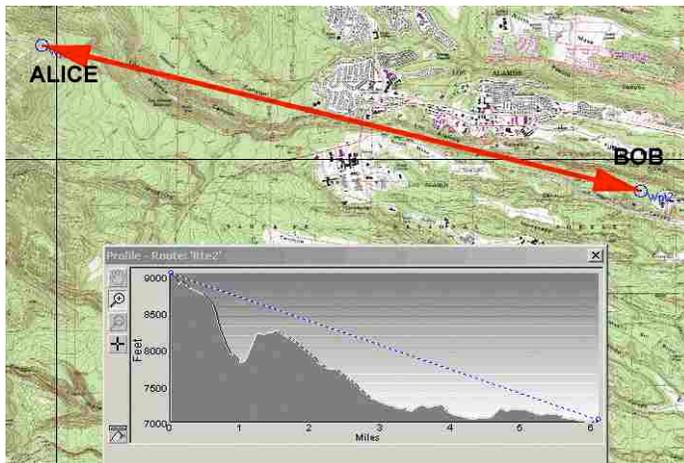
A: 11100010 00111101 10011111 10000111 11001111

B: 11100010 00111101 10011111 10000111 11001111



- key transferred by 772-nm single-photon communications
- 1-MHz sending rate; ~600-Hz key rate
- day: 45,576 secret bits/hour ; night: 113,273 secret bits/45 mins

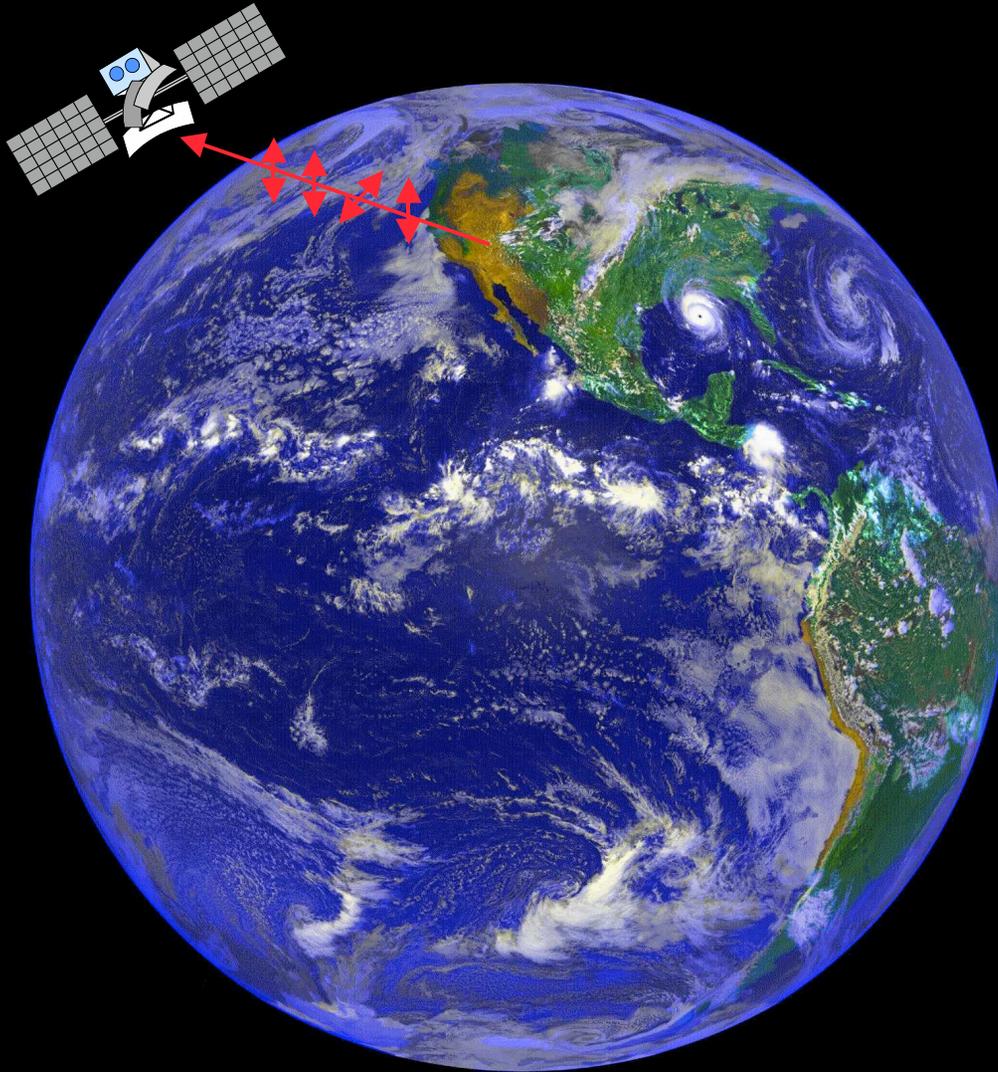
Receiver "Bob"



From Pajarito Mtn., Los Alamos, NM to TA53, Los Alamos National Laboratory

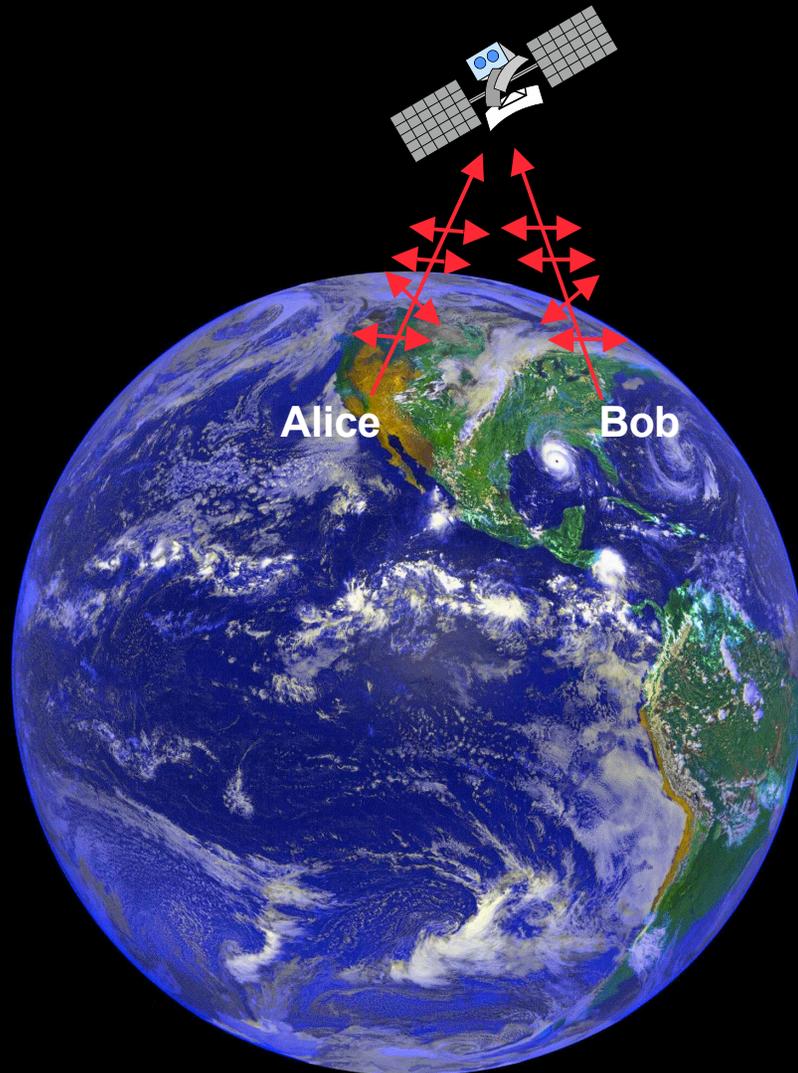


QKD for Satellite Communications



- on-orbit re-key offers long-term security guarantees with reliable security lifetime estimates
- key transfer between ground-based users
- cryptographically useful key rates possible

Satellite QKD for Long-Distance Key Generation?



- Alice and Bob generate quantum keys K_A and K_B with satellite
- satellite transmits $K_A \oplus K_B$ to Bob
 - tells Bob which bits to flip
- Bob computes
 - $(K_A \oplus K_B) \oplus K_B = K_A$
- Alice and Bob use K_A for encrypted communications

Los Alamos 48-km optical fiber quantum key distribution experiment

